



Attorney's Docket No. 032326-130

Handwritten: 7/11/05
AF/1/\$

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of)

Pascal Paillier)

Application No.: 09/818,658)

Filed: March 28, 2001)

For: METHOD FOR GENERATING)
ELECTRONIC KEYS FROM)
INTEGER NUMBERS PRIME)
WITH EACH OTHER AND A)
DEVICE FOR IMPLEMENTING)
THE METHOD)

Group Art Unit: 2134

Examiner: PIOTR POLTORAK

Appeal No.:

APPEAL BRIEF

Mail Stop APPEAL BRIEF - PATENTS

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Primary Examiner dated April 15, 2005, finally rejecting claims 1-9, which are reproduced as the Claims Appendix of this brief.

☒ A check covering the ☐ \$250.00 (2402) ☒ \$500.00 (1402)
Government fee is filed herewith.

☐ Charge ☐ \$250.00 (2402) ☐ \$500.00 (1402) to Credit Card. Form
PTO-2038 is attached.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

12/14/2005 JADD01 00000028 09818658

01 FC:1402

500.00 0P

Table of Contents

I.	Real Party in Interest.....	2
II.	Related Appeals and Interferences	2
III.	Status of Claims	2
IV.	Status of Amendments.....	2
V.	Summary Claimed Subject Matter.....	2
VI.	Grounds of Rejection to be Reviewed on Appeal.....	3
VII.	Argument	4
	A Claim 9: 35 U.S.C. § 112	4
	B. Claims 1-6: 35 U.S.C. § 103	4
	C. Claims 6-9: 35 U.S.C. § 103	7
VIII.	Claims Appendix	8
IX.	Evidence Appendix	8
X.	Related Proceedings Appendix.....	8

I. Real Party in Interest

The present application is assigned to Gemplus, a French corporation.

II. Related Appeals and Interferences

There are no known appeals, interferences or judicial proceedings which will affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims

The application contains claims 1-9, all of which are pending and stand finally rejected. This appeal is directed to claims 1-9.

IV. Status of Amendments

An Amendment was filed after the final Office Action on September 15, 2005, to address an objection to claim 5. Entry of the Amendment was refused in an Advisory Action dated October 19, 2005.

V. Summary Claimed Subject Matter

The claimed invention is directed to public key cryptography, and more particularly to the generation of cryptographic keys for encrypting and decrypting information. The security of public key cryptography is based upon the generation of the keys from two numbers that are prime numbers, or at least prime with respect to one another. To successfully generate the keys, therefore, two selected numbers must be tested to ensure that they are co-prime with one another.

Two numbers are co-prime if, and only if, their highest common factor (HCF) is 1. Several known techniques exist for calculating the HCF of two numbers with a microprocessor, as described in the specification at page 2, lines 8-16. However, these techniques are not well-suited for use on devices having limited processing

capabilities, such as smart cards, when dealing with the large numbers (e.g. 512 or 1024 bits) that are commonly employed in connection with public key cryptography protocols.

The claims are directed to a technique for generating cryptographic keys from two numbers, a and b , that employs a test for testing the co-primeness of a and b which is better suited to devices with limited processing and/or memory capabilities. An embodiment of this technique is illustrated in the flow chart of Figure 2. In this example, one of the numbers, b , is chosen in advance and stored in a register as a preliminary step. The other number, a , is chosen at random when the cryptographic protocol is to be executed. (Page 4, line 24, to page 5, line 1; page 5, line 27)

The test for co-primeness employs the Carmichael function $\lambda(n)$, which is described in the specification at page 5, lines 19-24. In the depicted example of Figure 2, the value $\lambda(b)$, where b is the prestored number, is calculated and also stored in a register as a preliminary step. (Page 5, line 28 to page 6, line 4)

Thereafter, when the protocol is to be executed, a random number a is chosen, and the value $a^{\lambda(b)} \bmod b$ is calculated. The result of this calculation is then compared with the value 1, to see if they are equal. If so, the co-primeness of a and b has been verified, and these numbers are stored in a register for use with the cryptographic protocol. If there is no equality, a new random number a is chosen, and the process is repeated. (Page 6, lines 4-15)

VI. Grounds of Rejection to be Reviewed on Appeal

1. The rejection of claim 9 under 35 U.S.C. §112, second paragraph, as being indefinite.
2. The rejection of claims 1-6 under 35 U.S.C. §103, as being unpatentable over the Lidl et al publication in view of the acknowledged state of the prior art and the Schneier publication.
3. The rejections of claims 6-9 under 35 U.S.C. §103, as being unpatentable over the Lidl et al publication in view of the acknowledged state of the prior art and the Schneier publication, and in further view of the Murphy et al patent.

VII. Argument

A. Claim 9: 35 U.S.C. § 112

Claim 9 was rejected under the second paragraph of 35 U.S.C. §112, as being indefinite. In paragraph 17, the final Office Action quotes the preamble of claim 9, and then states "the purpose of the limitation (above) is not understood...." It is not clear from the Office Action what is considered to be indefinite about the claim. The preamble of claim 9 is not intended to serve as a limitation. Claim 9 is a dependent claim, and pursuant to the requirements of 37 C.F.R. §1.75(c) comprises two parts, which respectively refer back to and further limit another claim in the application. The preamble, namely the recitation "the portable electronic device of claim 6" comprises the portion of the claim that refers back to another claim. The remainder of the claim, beginning with the "wherein" statement, comprises the portion that further limits the subject matter of claim 6. Specifically, claim 9 recites an additional function that is performed by the arithmetic processor defined in claim 6, namely the generation of a pair of cryptographic keys from the integers a, b.

The Office Action does not indicate why claim 9 is considered to be indefinite under the requirements of 35 U.S.C. §112, second paragraph. In the response to this rejection, Appellant explicitly requested that, if the rejection is maintained, the examiner explain the basis therefore, so that Appellant could be apprised of any amendments that may be necessary to overcome the rejection. However, no such explanation was provided in the Advisory Action.

B. Claims 1-6: 35 U.S.C. § 103

Claims 1-6 stand finally rejected under 35 U.S.C. § 103 on the grounds that they are considered to be unpatentable over the article by Lidl and Pilz entitled "Applied Abstract Algebra", in view of the prior art described in the background portion of the application and the Schneier publication, for the reasons presented in the initial Office Action dated September 22, 2004. In that prior Office Action, the Lidl publication was cited for its disclosure of generating RSA keys, and the statement on page 290 of the publication that:

It can be shown that $a^{\lambda(n)} \equiv 1 \pmod{n}$ where $\lambda(n)$ is the maximum period of the multiplicative group Z_n . Here, $\lambda(n)$ is called the *Carmichael function* ...

The initial Office Action acknowledged that the Lidl publication does not teach the step of verifying the co-primeness of the numbers a and n in this expression, and relies upon the Background portion of the present specification for such a teaching. The motivation for combining these two teachings is said to come from the Schneier publication, particularly the last section on page 258.

MPEP 2143 sets forth three fundamental requirements for a prima facie case of obviousness. The third one of the cited criteria is that "the prior art reference (or references when combined) must teach or suggest all the claim limitations." The rejection of claims 1-6 fails to meet this requirement.

The cited pages of the Lidl et al. publication pertain to the RSA public-key cryptosystem. At page 290, the publication provides a definition of the Carmichael function $\lambda(n)$, which is a classical object in number theory. The main property of this function is set forth on page 291. This property states that, for any two numbers a and n , raising a to some power k , or to some other power $k' = k + \text{a multiple of } \lambda(n)$, will yield the same result, modulo n , as long as k is different from 0 and n is not divisible by a $(k+1)$ th power.

The claimed invention exploits a different property of the Carmichael function which, in a sense, corresponds to the case $k=0$ that is excluded by the above-stated property. The invention is based on the proposition that raising any number a to the power $\lambda(n)$, modulo n , yields a value of 1 if, and only if, the number a is co-prime to n . This is a different property from the one described above, and in the Lidl et al. publication.

The objective of the invention is, for some number n given together with $\lambda(n)$, to randomly select a number a from among all the numbers that are co-prime to n . In accordance with this objective, successive random values are generated and checked for co-primality with n by using the second property of the Carmichael function as the test for co-primality. This claimed feature is not suggested by the cited prior art.

The rejection of the claims notes that the Lidl et al. publication discloses the property $a^{\lambda(n)} = 1 \pmod{n}$. What the reference does not teach, however, is that this property can be used to determine whether n is co-prime to a . The initial Office Action acknowledged that the Lidl patent does not contain such a teaching. In fact, in the context of the Lidl publication, a and n are not the numbers whose co-primeness is of concern. Rather, the co-prime numbers are designated as p and q . The number n is the product of these two co-prime numbers, i.e. $n = pq$. See the first full paragraph on page 289 following Example 2.16.

The rejection relies upon the prior art described in the specification, as well as the Schneier publication, to show that it is known to test for co-primality between two randomly chosen numbers. However, neither these examples of the prior art, nor the Lidl et al. publication, teach the *specific* test for co-primeness that is recited in the claims. Appellant is not attempting to claim the Carmichael function, per se, nor the general concept of testing for co-primality when selecting numbers to be used for cryptographic keys. Rather, the claims are directed to a *particular* test that is based upon the second noted property of the Carmichael function.

The cited prior art does not disclose this claimed subject matter, whether considered individually or in combination. The prior art described in the specification and the Schneier publication disclose the desirability of testing for co-primality. However, they do not disclose a test that is based upon a property of the Carmichael function. The Lidl et al. publication describes the Carmichael function. However, it does not disclose that a particular property of that function can be used as the test for co-primality. The final Office Action does not identify any nexus between the desirability of testing for co-primality on the one hand, and Lidl's disclosure of the Carmichael function on the other hand. There is no teaching in any of the references which leads a person of ordinary skill to utilize the claimed property of the Carmichael function as a test for co-primality when selecting pairs of numbers for the generation of cryptographic keys.

With specific reference to claims 1, 5 and 6, the combined disclosures of the references do not suggest the steps of selecting two numbers a and b to test for co-primeness, calculating the modular exponentiation $a^{\lambda(b)} \pmod{b}$, verifying whether this

modular exponentiation equals 1 (to determine whether the integers a and b are co-prime), and generating cryptographic keys from the integers a and b when the equality is verified. In particular, they do not suggest the conditional steps of “reiterating operations A and B with another pair of integers when the modular exponentiation **is not** equal to 1” and “generating at least two cryptographic keys from the integers a and b when the equality **is** verified”, as recited in claim 1. Nor do they teach the analogous steps of claims 5 and 6. As such, the cited prior art does not “teach or suggest all the claim limitations” as required for a *prima facie* case of obviousness.

Furthermore, in connection with claim 6, there has been no showing where the Lidl publication, the acknowledged prior art, or the Schneier publication disclose a portable electronic device, comprising an arithmetic processor and an associated program memory, which performs the operations recited in the claim. In fact, in Paragraph 29 of the initial Office Action, the examiner explicitly stated that these three references do not contain any such teaching. For this additional reason, claim 6 is not rendered unpatentable by the cited prior art.

C. Claims 6-9: 35 U.S.C. § 103

In view of the express acknowledgement set forth immediately above, the rejections of claims 6-9 appearing in Paragraphs 21 and 22 of the final Office Action rely upon the Murphy et al patent (US 6,226,744) for its disclosure of a smart card having an on-board math coprocessor to generate keys. However, there is no teaching in the Murphy patent that overcomes the differences noted in the foregoing discussion of claims 1-6. Specifically, there is no disclosure suggesting that the keys are generated from two numbers that are selected and tested for co-primeness by means of the operations recited in steps A-D of claim 6.

Again, therefore, even when the Murphy patent is considered, the cited prior art fails to meet the requirement that it “teach or suggest all the claim limitations.”

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

(none)

X. Related Proceedings Appendix

(none)

CONCLUSION


As demonstrated in the preceding arguments, the cited prior art does not "teach or suggest all the claim limitations", as is required for a prima facie case of obviousness. In addition, the final Office Action has not identified any indefiniteness in the language of claim 9.

The rejections of the claims are not properly founded in the statute, and should be reversed.

Respectfully submitted,
Buchanan Ingersoll PC

Date December 13, 2005

By:


James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

VIII. CLAIMS APPENDIX

The Appealed Claims

1. A method for generating cryptographic keys from two integers a , b that are co-prime with one another, which includes the following operations:

- A) - calculating the modular exponentiation $a^{\lambda(b)} \bmod b$, where λ is the Carmichael function,
- B) - verifying whether this modular exponentiation is equal to 1,
- C) - reiterating operations A and B with another pair of integers when the modular exponentiation is not equal to 1; and
- D) - generating at least two cryptographic keys from the integers a and b when the equality is verified.

2. A method for generating electronic keys according to Claim 1, wherein:

- an integer number b with a given length is chosen and is stored in memory,
- an integer number a is drawn at random,
- $a^{\lambda(b)} \bmod b$ is calculated,
- it is verified that $a^{\lambda(b)} = 1 \bmod b$ (or $a^{\lambda(b)} \bmod b = 1$),
- the number a is stored in memory in the case where equality is verified,
- the above steps are reiterated with another number a when equality is not verified.

3. A method for generating electronic keys according to Claim 1, wherein the integer b is predetermined, and the value $\lambda(b)$ is calculated in advance and stored in memory.

4. The method of claim 1 further including the steps of encrypting and/or decrypting information by means of a public key cryptography protocol, using said cryptographic keys as the encryption and decryption keys.

5. A method for generating RSA or El Gamal or Schnorr cryptographic keys, comprising the steps of:

- A) - selecting two integers a , b as candidates;
- B) - calculating the modular exponentiation $a^{\lambda(b)} \bmod b$, where λ is the Carmichael function,
- C) - verifying whether this modular exponentiation is equal to 1,
- D) - retaining the pair a , b when equality is verified,
- E) - reiterating steps B and C with another pair of numbers when the modular expansion is not equal to 1, and
- F) - generating at least pair of cryptographic keys from the pair a , b retained in step D.

6. A portable electronic device comprising an arithmetic processor and an associated program memory that are capable of effecting modular exponentiations, and further including a program for verifying the co-primeness of integer numbers of given length, which performs the following operations:

- A) - calculating the modular exponentiation $a^{\lambda(b)} \bmod b$, where λ is the Carmichael function,
- B) - verifying that this modular exponentiation is equal to 1,
- C) - storing the pair a , b in the arithmetic processor when equality is verified, and
- D) - reiterating steps A and B with another pair of integers when equality is not verified.

7. A portable electronic device according to Claim 6, wherein the number b is predetermined and the value $\lambda(b)$ is calculated in advance and stored in a memory.

8. A portable electronic device according to Claim 6, wherein said portable electronic device comprises a chip card with a microprocessor.

9. The portable electronic device of claim 6 wherein said arithmetic processor generates a pair of cryptographic keys from the stored pair of integers a, b.